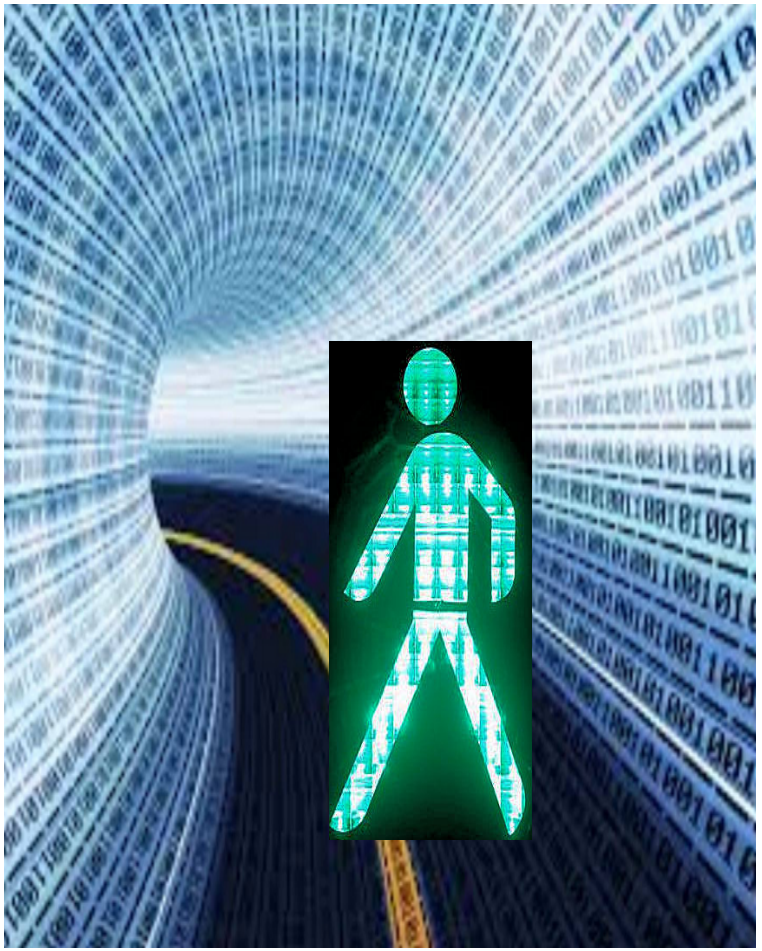
Crossing the Digital Street

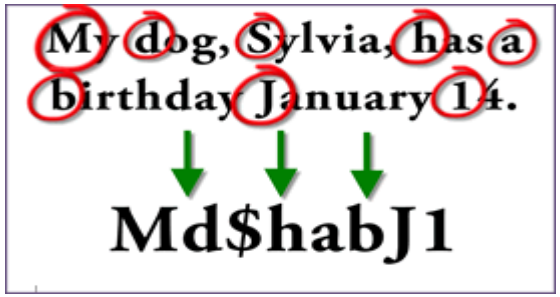
AMC/A6OS
DSN 779-6298

Stop. Think. Connect. Before You Cross The Digital Street

- Cyber criminals do not discriminate; they target vulnerable computer systems regardless of whether they are part of a large corporation, a small business, or belong to a home user.
- Cybersecurity is a shared responsibility in which all Americans have a role to play.
- The three facets of the message are:
  - ✓ **STOP:** Before you use the Internet, take time to understand the risks and learn how to spot potential problems.
  - ✓ **THINK:** Take a moment to be certain the path ahead is clear. Watch for warning signs and consider how your actions online could impact your safety or your family's.
  - ✓ **CONNECT:** Enjoy the Internet with greater confidence, knowing you've taken the right steps to safeguard yourself and your computer.



Password Passage



Protect Your Passwords

- **Make passwords long and strong:** Combine capital and lowercase letters with numbers and special characters to create a more secure password. Change any default passwords on your mobile device to ones that would be difficult for someone to guess.
- **Create a passphrase:** Passwords can now be "mybosslikesreadingcartoonsinthenewspaper."
- **Unique account, unique password:** Use different passwords for different programs and devices to thwart cybercriminals. Do not choose options that allow your device to remember your passwords.
- **Write it down and keep it safe:** Everyone can forget a password. Keep a list that's stored in a safe, secure place away from your computer.
- **Get Two Steps Ahead:** Turn on two-factor authentication – on accounts where available. Two-factor authentication can use anything from a text message to your phone to a token to a biometric like your fingerprint to provide enhanced account security.

Device Drive

Keep a Clean Machine

- **Keep security software current:** Having the latest security software, web browser, and operating system are the best defenses against viruses, malware, and other online threats.
- **Automate software updates:** Many software programs will automatically connect and update to defend against known risks. Turn on automatic updates if that's an available option.
- **Plug & scan:** "USBs" and other external devices can be infected by viruses and malware. Use your security software to scan them.
- **Turn On Your Firewall:** Most OS's include a built-in firewall, which monitors incoming and outgoing connections. A firewall won't provide complete protection, but it's a setting that should always be enabled.

Connection Court

Connect with Care

- **Get savvy about Wi-Fi hotspots:** Limit the type of business you conduct and adjust the security settings on your device to limit who can access your machine. Avoid automatically connecting to Wi-Fi hotspots.
- **Use HTTPS:** When banking and shopping, check to be sure the website is security enabled. Look for web addresses with “https://”, which means the site takes extra measures to help secure your information. “http://” is not secure.
- **Turn Off Sharing:** Disable sharing settings for your music library, printers or files before connecting to a public Wi-Fi network or ANYONE may be able to hack into your PC.
- **Use a VPN:** The most secure way to browse on a public network is to use a virtual private network. A VPN routes your traffic through a secure network even on public Wi-Fi, giving you all the perks of your private network while still having the freedom of public Wi-Fi.

WWW Way

I,
ME,
MYSELF
A BRAND !!

Be Web Wise

- **Stay current:** Keep pace with new ways to stay safe online: Check trusted websites for the latest information, and share with friends, family, and colleagues and encourage them to be web wise.
- **Think before you act:** Be wary of communications that implores you to act immediately, offers something that sounds too good to be true, or asks for personal information.
- **Own your online presence:** When available, set the privacy and security settings on websites to your comfort level for information sharing. It's ok to limit how and with whom you share information.
- **Protect all devices that connect to the Internet:** Along with computers… smart phones, gaming systems, and other web-enabled devices also need protection from viruses and malware.
- **Back up your information:** Back up your contacts, photos, videos and other mobile device data with another password protected device or cloud service.

Email Trail

To Mail Or Not To Mail???

- **When in doubt, throw it out:** Links in email, tweets, posts, and online advertising are often the way cybercriminals compromise your computer. Delete emails that are suspicious (Phishing) or are from unknown sources. Even if you know the source, it's best to delete or if appropriate, mark as junk email.
- **Use a Spam filter:** Spam filters help you keep spam emails from your inbox or flag spam emails as such so that you are aware of them.
- **Digitally sign and encrypt your e-mails:** Any PII (Personal Identifiable Information) or organization proprietary information can be used by Cybercriminals to impersonate you.
- **Remember to log out/sign out**: Especially if you're using a public computer, such as at the library or an Internet cafe, and close the browser. It's quick, easy, and may save your Email account from unwanted trespassers.

Social Superhighway

Be a Good Online Citizen

- **Safer for me more secure for all:** What you do online has the potential to affect everyone – at home, at work and around the world. Practicing good online habits benefits the global digital community.
- **Post only about others as you have them post about you:** The Golden Rule applies online as well.
- **Help the authorities fight cyber crime:** Report stolen finances or identities and other cybercrime to the Internet Crime Complaint Center (www.ic3.gov) and to your local law enforcement or state attorney general as appropriate.
- **Keep personal info personal:** Use your personal profile to keep your real friends (the ones you know trust) more synched up with your daily life.

Personal Information Highway

Protect Your Personal Information

- **Personal Information Is Like Money. Value It. Protect It.:** Information about yourself, such as games you like to play, has value – just like money. Be selective with the information you provide to emails, apps, websites and social media sites.
- **Do not provide personal information:** Make certain of a person's or organization's authority to have your Personal Identifiable Information (PII).
- **Guard your mobile device:** To prevent theft and unauthorized access or loss of sensitive information, never leave your mobile devices–including any USB or external storage devices–unattended in a public place. Keep your devices secured in taxis, at airports, on airplanes, and in your hotel room.
- **Keep it locked:** Get into the habit of locking your device when you are not using it. Even if you only ste

U.S. AIR FORCE

References

This brief and additional Information can be found here:

https://eim.amc.af.mil/sites/Cyber/default.aspx

Air Force Instruction 33-200 (31AUG15)
www.e-publishing.af.mil

POC: AMC/A6OS
DSN 779-6298